CLAIMS

WHAT IS CLAIMED IS:

1. A method for automatically directing network connections based on access rights possessed by a user of a wireless terminal, the method comprising:

receiving a certificate, having security information indicative of the access rights possessed by the user, from the wireless terminal;

determining whether the received certificate corresponds to a service provider authentication certificate which identifies access rights for a targeted service;

directing the network connection to the targeted service if the received certificate corresponds to the service provider authentication certificate; and

directing the network connection to an enrollment module to register for the service provider authentication certificate, if the received certificate does not correspond to the service provider authentication certificate.

2. The method of Claim 1, further comprising providing a list of one or more available predetermined certificates to the wireless terminal.

3. The method of Claim 2, further comprising providing the list of available predetermined certificates to the wireless terminal in a predetermined order in which selection at the wireless terminal is to be effected.

4. The method of Claim 3, further comprising selecting, at the wireless terminal, a locally-stored certificate corresponding to the highest order predetermined certificate that matches the locally-stored certificate.

5. The method of Claim 4, further comprising establishing the network connection using the selected locally-stored certificate, wherein the selected certificate is the certificate received from the wireless terminal having security information indicative of the access rights possessed by the user.

6. The method of Claim 3, further comprising allowing the wireless terminal to establish the network connection utilizing a locally-stored certificate corresponding to the predetermined certificate that is highest in the predetermined order that matches the locally-stored certificate.

7. The method of Claim 1, wherein receiving a certificate comprises receiving the certificate via a client certificate message issued by the wireless terminal.

8. The method of Claim 1, further comprising enrolling the user with the targeted service via the enrollment module when the network connection is directed to the enrollment module.

9. The method of Claim 8, further comprising providing the service provider authentication certificate back to the wireless terminal in response to enrolling the user with the targeted service.

10. The method of Claim 1, wherein the access rights possessed by the user are stored as local certificates on a Wireless Identity Module (WIM).

11. The method of Claim 1, further comprising supplying the wireless terminal with a list of available authentication certificates from which the wireless terminal may use to establish the connection.

12. The method of Claim 11, further comprising supplying the wireless terminal with the list of available authentication certificates in a preferred order from which the wireless terminal must utilize a highest preference authentication certificate possessed at the wireless terminal in establishing the connection.

13. The method of Claim 12, wherein the highest preference authentication certificate listed is the service provider authentication certificate.

14. The method of Claim 11, wherein determining whether the received certificate corresponds to a service provider authentication certificate comprises comparing the received certificate to the list of available authentication certificates.

15. The method of Claim 1, wherein determining whether the received certificate corresponds to a service provider authentication certificate comprises comparing the received certificate to the service provider authentication certificate.

16. A system for managing access and enrollment for a secure service available to a user via a wireless terminal, comprising:

a service module from which a service provider avails the secure service to the user of the wireless terminal;

an enrollment manager to effect user registration to the secure service; and

a switch module coupled to receive a security certificate utilized by the wireless terminal in establishing a connection therewith, wherein the switch module directs the connection to either the service module or the enrollment manager depending on the security certificate utilized in establishing the connection.

17. The system as in Claim 16, wherein the switch module determines which security certificate is utilized in establishing the connection, and directs the connection to either the service module or the enrollment manager depending on the utilized security certificate.

18. The system as in Claim 17, wherein the security certificate is digitally signed by the service provider indicating that the user is registered with the service provider for use of the secure service, thereby directing the connection to the service module.

19. The system as in Claim 17, wherein the security certificate is not digitally signed by the service provider, indicating that the user is not registered with

the service provider for use of the secure service, thereby directing the connection to the enrollment manager.

20. The system as in Claim 17, wherein the security certificate is digitally signed by a trusted authority that is trusted by the service provider, indicating that the user may obtain registration through the trusted authority, thereby directing the connection to the enrollment manager.

21. The system as in Claim 16, wherein the security certificate comprises an authentication certificate.

22. The system as in Claim 21, wherein the authentication certificate comprises at least one of an identity verification authentication certificate, an authorization certificate, and a non-repudiation certificate.

23. The system as in Claim 16, wherein the switch module comprises a list of potential authentication certificates listed in a preferred order of use, and wherein the switch module provides the list of potential authentication certificates to the wireless terminal to allow the wireless terminal to establish the connection using a highest order authentication certificate in accordance with the preferred order of use.

24. The system as in Claim 23, wherein the switch comprises a compare module to compare at least one of the predetermined authentication certificates to the authentication certificate used by the wireless terminal.

25. The system as in Claim 24, wherein:

(a) the compare module compares a service provider's authentication certificate to the authentication certificate used by the wireless terminal in establishing the connection;

(b) if a match is found, the switch module directs the user to the service module to use the secure service; and

(c) if a match is not found, the switch module directs the user to the enrollment manager to effect user registration to the secure service.

26. The system as in Claim 24, wherein:

(a) the compare module compares each of the predetermined authentication certificates to the authentication certificate used by the wireless terminal; and

(b) the switch module directs the user to the service module or the enrollment manager depending on the results of the comparison.

27. The system as in Claim 16, wherein the enrollment manager is configured to issue authentication certificates upon successful registration, including the service provider authentication certificate required for use with the secure service.

28. A system for managing user access and enrollment for a secure service available on a network, comprising:

a wireless network including a plurality of wireless terminals operable therein;

a network of computing systems wherein at least one of the computing systems comprises a server computing system hosting a secure service targeted by at least one of the wireless terminals, and wherein at least one of the computing systems comprises an enrollment server to effect user registration to the secure service;

a gateway computing system configured to bridge communications between the wireless network and the network of computing systems; and

a network switch coupled to receive an authentication certificate utilized by a wireless terminal in establishing a connection with the network of computing systems, wherein the network switch switches the connection to the server computing system or the enrollment server depending on the authentication certificate utilized by the wireless terminal in establishing the connection.

29. The system as in Claim 28, wherein the gateway computing system comprises a Wireless Application Protocol (WAP) gateway, and at least the wireless terminal establishing the connection with the network of computing systems comprises a WAP-compliant terminal.

30. The system as in Claim 29, wherein the WAP-compliant terminal comprises one of a wireless telephone, personal digital assistant, wireless pager, and wireless laptop computer.

31. The system as in Claim 28, wherein the network of computing systems comprises the Internet, and wherein the Wireless Application Protocol (WAP) is used to communicate between the wireless terminal and the Internet.

32. A system for automatically routing network connections based on access rights possessed by a user of a wireless terminal, comprising:

means for receiving a certificate, having security information indicative of the access rights possessed by the user, from the wireless terminal;

means for determining whether the received certificate corresponds to a service provider authentication certificate which identifies access rights for a targeted service; and

means for directing the network connection to the targeted service if the received certificate corresponds to the service provider authentication certificate, and for directing the network connection to an enrollment module to register for the service provider authentication certificate if the received certificate does not correspond to the service provider authentication certificate.

33. A computer-readable program storage medium tangibly embodying a program of instructions executable by a computing system to manage user access and enrollment for secure network services by performing steps comprising:

receiving a certificate, having security information indicative of the access rights possessed by the user, from the wireless terminal;

determining whether the received certificate corresponds to a service provider authentication certificate which identifies access rights for a targeted service;

directing the network connection to the targeted service if the received certificate corresponds to the service provider authentication certificate; and

directing the network connection to an enrollment module to register for the service provider authentication certificate, if the received certificate does not correspond to the service provider authentication certificate.